

General facts about groups.

(S): A semigroup consists of a set \mathcal{G} together with a law of combination which satisfies the associative law. With each ordered pair (a, b) in $\mathcal{G} \times \mathcal{G}$ there is associated an element $c = f(a, b)$ of \mathcal{G} . If $f(a, b) = f(b, a)$ for all a, b in \mathcal{G} then the group is said to be commutative, or Abelian. In the general theory here, it is convenient to denote $f(a, b)$ by simple juxtaposition: $c = f(a, b) = ab$. The associativity means that $a(bc) = (ab)c$ whenever a, b, c are in \mathcal{G} . So we just write this as abc .

(G): A semigroup is a group if all linear equations in \mathcal{G} are solvable, that is, if a, b are in \mathcal{G} , then there are x, y

in \mathcal{G} with $ax = b$ and $ya = b$.

Examples.

- ① \mathcal{G} = real valued functions defined on $(-\infty, +\infty)$

Law of combination = composition

$$fg := f \circ g,$$

with

$$(f \circ g)(x) := f(g(x)).$$

This forms a semigroup. Composition of functions is always associative! Check it out.

- ② The subset of the above \mathcal{G} of continuous functions of that \mathcal{G} . We know that f and g continuous $\Rightarrow f \circ g$ continuous. This is key, for the law of combination rule says that $f \circ g$ must again be in \mathcal{G} ! In math these

functions are denoted by $C(-\infty, +\infty)$. Similarly, $C^n(-\infty, +\infty)$, the n times continuously differentiable functions on $(-\infty, +\infty)$, form a semigroup with respect to the operation of composition of functions, by the chain rule applied inductively. But what subsets of $C^n(-\infty, +\infty)$ also form groups? This must not be hard; it must have something to do with "inversion".

③ $M = C^{n \times n}$, the complex $n \times n$ matrices.

Law of combination = matrix multiplication:

$$C = AB.$$

This represents composition of linear transformations.

e.g.

$$A: \mathbb{C}^n \rightarrow \mathbb{C}^n$$

$$x \rightarrow y := Ax,$$

so it's automatically associative.

But the closure requirement, i.e. the law of composition, holds because the product of A and B in $\mathbb{C}^{n \times n}$ is also in $\mathbb{C}^{n \times n}$!

For $\mathcal{A} = \mathbb{C}^{n \times n}$ and the operation of matrix multiplication, the group condition G means that the equations $AX = B$ and $YA = B$ have solutions X and Y in \mathcal{A} whenever A and B are given, in \mathcal{A} . But matrix (semi-) groups are special.

By the reverse order rule for ~~multiplication~~ ^{conjugate transposition}, $YA = B \Leftrightarrow$

$$A^H Y^H = B^H. \text{ The statement}$$

that $AX = B$ is always solvable, for every A and B in \mathcal{J} , just means, on equating columns, that $Ax_j = b_j$, $j = 1, 2, \dots, n$, are always solvable. By definition of the range of A ,

$$\mathcal{R}(A) := \{y = Ax : x \in \mathbb{C}^n\}$$

this means that

$$\mathcal{R}(A) = \mathbb{C}^n.$$

Likewise, $A^H Y^H = B^H$ always solvable \iff

$$\mathcal{R}(A^H) = \mathbb{C}^n.$$

Now, by Gauss (factorization) by golly, or by using the "wretched" form,

$$\mathcal{R}(A) = \mathbb{C}^n$$

\iff

$$p = \# \text{ pivots} = n$$

\iff

$$\begin{aligned} v &= \# \text{ free variables} \\ &= n - p = 0 \end{aligned}$$



$$\begin{aligned} \mathcal{N}(A) &:= \text{null space of } A \\ &:= \{x \text{ in } \mathbb{C}^n : Ax = 0\} \\ &= \{0\} \end{aligned}$$

↔ solutions of $Ax = b$, if they exist, are unique.

Now the number p of pivots is independent of the pivot strategy, and depends only on the matrix A . So we define

$$\rho(A) := \text{rank } A := p$$

and

$$\nu(A) := \text{null } A := n - p$$

to be the rank and nullity of A , respectively.

I say that an $n \times n$ matrix is nonsingular if $Ax = b$ is always uniquely solvable; for every b there is exactly one solution x .

Since $A: \mathbb{C}^m \rightarrow \mathbb{C}^n$ this means that

$$\mathcal{R}(A) = \mathbb{C}^m \text{ and } \eta(A) = \{0\},$$

and that

$$\rho = \# \text{ pivots} = m = n.$$

So, nonsingular matrices must be square: $m = n$. And

now

A in $\mathbb{C}^{n \times n}$ nonsingular

\Leftrightarrow

$$\rho = \rho(A) = n$$

\Leftrightarrow

$$\mathcal{R}(A) = \mathbb{C}^n$$

\Leftrightarrow

$Ax = b$ always solvable

\Leftrightarrow

$$\eta(A) = \{0\}$$

\Leftrightarrow

$$Ax = 0 \Rightarrow x = 0$$

\Leftrightarrow

solutions of $Ax = b$ unique.

But the group axiom G also demands that $A^H Y^H = B^H$ be always solvable for Y^H , given A^H and B^H . But, at a lower level, this just means that $A^H z = c$ is always solvable for z , given c . As above, with $A \leftrightarrow A^H$, this is true if and only if A^H is non-singular $\Leftrightarrow \rho(A^H) = n \Leftrightarrow \mathcal{R}(A^H) = \mathbb{C}^n$, $\Leftrightarrow A^H z = c$ always solvable $\Leftrightarrow \mathcal{N}(A^H) = \{0\} \Leftrightarrow (A^H z = 0 \Rightarrow z = 0) \Leftrightarrow$ solutions of $A^H z = c$ unique. So the punch line is that

$$\rho(A^H) \geq \rho(A)$$

i.e.

$$\text{rank } A \geq \text{rank } A^H.$$

This follows from the (builtin!) "duality" of Gauss factorization: if

$$Q^T A P = L U = \underbrace{\begin{bmatrix} \ddots & & \\ & \square & \\ & & \ddots \end{bmatrix}}_P \begin{bmatrix} \square & \\ & \square \end{bmatrix} P$$

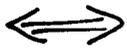
with P and Q (real) permutation matrices, then

$$P^T A^H Q = U^H L^H = \underbrace{\begin{bmatrix} \times & & \\ & \times & \\ & & \times \end{bmatrix}}_{\rho = \rho(A^H) = \rho(A)} \{ \square \} P,$$

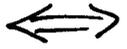
and vice versa. L is unit lower trapezoidal (1s on the main diagonal), U has the (nonzero) pivots on its main diagonal. It's important only that these diagonal elements be nonzero.

Bottom line. $\mathbb{C}^{n \times n}$ is a semigroup under matrix multiplication. The subset $GL(n, \mathbb{C})$ of nonsingular matrices in $\mathbb{C}^{n \times n}$ forms a group, called the general linear group. Moreover,

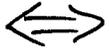
$$\begin{aligned} & A \text{ in } \mathbb{C}^{n \times n} \text{ nonsingular} \\ \iff & \rho = \rho(A) = n, \quad \text{main practical test} \end{aligned}$$



$$\mathcal{R}(A) = \mathbb{C}^n$$



$$\eta(A) = \{0\}$$



$$Ax = 0 \Rightarrow x = 0 \quad \begin{array}{l} \text{main} \\ \text{theoretical} \\ \text{test} \end{array}$$



$$\mathcal{R}(A^H) = \mathbb{C}^n$$



$$\eta(A^H) = \{0\}$$



$$\det A \neq 0$$

relatively
useless, in
practice!

$$\square \det A := (-1)^\nu u_{11} u_{22} \dots u_{nn}$$

if $p = n$, with the u_{kk} the pivots and $\nu = \#$ interchanges (of rows and/or columns), and

$$\det A := 0 \text{ if } p < n. \quad \blacksquare$$

The reason $\det A$ is useless for real problems is that, even for moderate n , it varies wildly as a function of the matrix elements. Moreover, usually, theoretical things

which use determinants can be done better another way!

More general group theory.

Axiom G \Rightarrow axiom 1.

1. There's a right identity element e in \mathcal{G} , with $ae = a$ for all a in \mathcal{G} .

□ First, fix c in \mathcal{G} , and let e solve $ce = c$, so e is an identity element for c . Now, for any a in \mathcal{G} let x solve $xc = a$. Then $ae = xce = xc = a$, so e is a right identity element for every a in \mathcal{G} . ■

Axiom G \Rightarrow axiom 2.

2. Each element a in \mathcal{G} has a right inverse element b in \mathcal{G} , with $ab = e$.

□ Solve $ax = e$ for $x =: b$. ■

We'll eventually show that axioms 1 and 2 \Rightarrow axiom 6. Groups are most often defined using axioms 1 and 2, but I like the equation solving aspect of axiom 6.

Axiom 2 \Rightarrow axiom 3

3. Any right inverse, with respect to such an e , is also a left inverse, and is thus a two sided inverse.

□ Given a , let $ab = e$. Since b is in \mathcal{G} there's a c in \mathcal{G} with $bc = e$. So, $ba = bae = babc = bec = bc = e!$ ■

Axioms 1, 2, 3 \Rightarrow axiom 4

4. Right identity elements, with respect to such an e , are also left identity elements.

□ Suppose $ae = a$ for all a in \mathcal{G}

613

(axiom 1). Pick a in \mathcal{G} and let $ab = e$ (axiom 2). By axiom 3 also $ba = e$. Then, $ea = aba = ae = e$, as required. \blacksquare

Axioms 1, 4 \Rightarrow axiom 5.

5. The (two sided) identity element e is unique.

\square Suppose e_1, e_2 right identity elements, guaranteed by axiom 1. By axiom 4 e_1 and e_2 are also left identity elements. So $e_1 = e_1 e_2 = e_2 =: e$. \blacksquare

Axioms 2, 3, 4 \Rightarrow axiom 6.

6. (Right) inverse elements are unique. Hence each a in \mathcal{G} has a unique (two sided) inverse element, a^{-1} , with

$$aa^{-1} = e = a^{-1}a.$$

\square Suppose $ab = ac = e$ (#2).

By #3, $ba = ca = e$. By these and #4, $b = eb = bab = bac = ec = c$. ■

Axiom 6 \Rightarrow axiom 7.

7. a, b in $\mathcal{H} \Rightarrow (ab)^{-1} = b^{-1}a^{-1}$,
reverse order rule for inversion.

□ $ab \cdot b^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$, so
 $(ab)^{-1} = b^{-1}a^{-1}$ by the uniqueness of inverses. ■

Axioms 1, 2, 3, 4 \Rightarrow axiom 8

8. The equations $ax = b$ and $ya = b$ are always uniquely solvable.

□ $ax = b$ is solved by $x = a^{-1}b$, since $ax = aa^{-1}b = eb = b$. This uses #s 1, 2 and 4. x is unique because there's a formula for it. $x = a^{-1}b$ expresses the solution x as a (single valued!) function of a and b . For this it is key that

a^{-1} is uniquely determined by a . However, to be pedantic, if $ax_0 = ax_1 = b$ then $x_0 = ex_0 = a^{-1}ax_0 = a^{-1}ax_1 = ex_1 = x_1$, using #s 1, 2, 3, 4. Similarly, $y = ba^{-1}$ is the unique solution of $ya = b$. ■

Finally, to complete the circle,

Axiom 8 \Rightarrow axiom 1.

□ Trivial. ■

But, in 8, if $ax = b$ is always solvable, then so is $ya = b$ which, by 7, is equivalent with $a^{-1}y^{-1} = b^{-1}$. One might hope that

8' := 1', $ax = b$ is always solvable.

would be enough to imply 1 and 2. Apparently not! But it is enough in $GL(n, \mathbb{C})$, where #1 means any of many equivalent characterizations of nonsingular matrices A .

One thing did come out of this,
that for A, B in $\mathbb{C}^{n \times n}$,

$$AB = I \implies BA = I,$$

or equivalently,

$$BA = I \implies AB = I.$$

I call this one side is enough. It is too often overlooked. It seems pretty practical to me. Here it took a lotta "group theory" to get it. This is not "unuseful". But I prefer the way in my "Gauss factorization" notes, which seems to me to be more down to Earth and related with the practical problems of linear equation solving. Missing here is that $\text{rank } A = \rho(A)$ is independent of the pivot strategy. That's a key fact of Linear Algebra, and is not hard. It's in my "GF" notes, 3 times!